Corrigé

Exercice 1

1) Soit $P := X^n Y^n + (Y+1)(X+1) \in \mathbb{Z}[X,Y] = (\mathbb{Z}[X])[Y]$

Appliquons le th d'Eisenstein dans l'anneau factoriel $A = \mathbb{Z}[X]$ et l'élément irréductible $Q = X+1$. (car de degré 1 et de contenu 1).

- Q divise les coefficients de $1, Y, Y^2, \dots, Y^{n-1}$
- Q ne divise pas le coefficient de Y^n
- Q^2 ne divise pas le coefficient de 1.

Donc P est irréductible dans $\mathbb{Q}[X][Y]$

Comme $\operatorname{pgcd}_{\mathbb{Z}[X]}(X^n, X+1) = 1$, P est de contenu 1

et donc P est irréductible dans $\mathbb{Z}[X][Y]$.

2) 1ère méthode : $\mathbb{F}_q^\times$ est un groupe de cardinal $q-1$ donc

$\forall x \in \mathbb{F}_q^\times$, $o(x) \mid q-1$ par le th de Lagrange.

Ainsi $\forall x \in \mathbb{F}_q^\times$, $x^{q-1} = 1$ d'où $x^q = x$. (*)

Cette identité est aussi satisfaite par $0 \in \mathbb{F}_q$.

Donc tous les q éléments de $\mathbb{F}_q$ sont des racines du polynôme $X^q - X \in \mathbb{F}_q[X]$.

Ce polynôme étant de degré q et unitaire, on en déduit $X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha)$.

Pour démontrer que $X^q - X \mid P^q - P$, il suffit donc de montrer que tous les éléments de $\mathbb{F}_q$ sont racine de $P^q - P$.

(les racines de $X^q - X$ sont simples!)

Or pour $x \in \mathbb{F}_q$, $P(x)^q = P(x)$ d'après (*).

et donc x est bien racine de $P^q - P$.

2ème méthode : $\mathbb{F}_q$ dans $\mathbb{F}_q[X]$, $P(X)^q = P(X^q)$.

Notons $P = a_0 + a_1 X + \dots + a_n X^n$ avec les $a_i \in \mathbb{F}_q$.

Comme $\mathbb{F}_q[X]$ est de caractéristique p, on a

$P(X)^p = (a_0 + a_1 X + \dots + a_n X^n) = a_0^p + a_1^p X^p + \dots + a_n^p X^{pn}$

puis par une récurrence immédiate

$P(X)^q = a_0^q + \dots + a_n^q X^{qn}$.

Enfin par (*), on a $\forall i, a_i^q = a_i$.

d'où $P(X)^q = a_0 + a_1 X^q + \dots + a_n (X^q)^n = P(X^q)$.

Mais alors dans $R = \mathbb{F}_q[X]/(X^q - X)$, on a $\overline{X}^q = \overline{X}$.

D'où $\overline{P(X)}^q = \overline{P(X^q)} = P(\overline{X}^q) = P(\overline{X}) = \overline{P(X)}$

On a donc par définition du quotient, $X^q - X \mid P^q - P$.

3) Soit $f : E \to F \in \mathcal{L}(E, F)$.
On distingue 2 cas :
- Soit $y \in \mathrm{Im}(f)$. Dans ce cas, $\forall y \; f^{-1}(y)$ est un espace affine de direction $\ker f \subset E$.
En effet, si $x_0 \in f^{-1}(y)$, on a $f^{-1}(y) = \{x_0 + k, \text{ avec } k \in \ker f\}$.

- Soit $y \notin \mathrm{Im}(f)$, dans ce cas $f^{-1}(y) = \emptyset$ est bien un espace affine par convention.

4) Soit $\mathcal{C}$ la conique d'équation
$$x^2 - y^2 + ax + by + c = 0.$$
Elle est non dégénérée ssi la forme quadratique
$Q : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto x^2 - y^2 + axz + byz + cz^2$ est non dégénérée.

ie ssi $\begin{pmatrix} 1 & 0 & a/2 \\ 0 & -1 & b/2 \\ a/2 & b/2 & c \end{pmatrix} \neq 0$ ie ssi $\left(-c - \frac{b^2}{4}\right) + \frac{a^2}{4} \neq 0$

ie $\Delta = a^2 - b^2 - 4c \neq 0$

L'équation de $\mathcal{C}$ se récrit :
$$\left(x + \frac{a}{2}\right)^2 - \left(y - \frac{b}{2}\right)^2 = \frac{a^2 - b^2 - 4c}{4} = \Delta.$$
Si $\Delta \neq 0$, c'est l'équation d'une hyperbole.
Si $\Delta \neq 0$ (à une homothétie près l'équation est de la forme $X^2 - Y^2 = 1$).

Si $\Delta = 0$, l'équation est de la forme $X^2 - Y^2 = 0$.
Ce qui est l'équation de 2 droites sécantes.

Exercice 2

1) Comme $[L : K] = n$, toute famille de $(n+1)$ éléments de L est liée par une relation linéaire non triviale à coeff dans K.
Ainsi, la famille $1, x, x^2, \dots, x^n$ est liée :
$\exists (a_0, \dots, a_n) \in K \setminus \{(0, \dots, 0)\}$ tq $a_0 + a_1 x + \dots + a_n x^n = 0$.
En posant $P = a_0 + a_1 X + \dots + a_n X^n$, on a $P(x) = 0$ et $P \neq 0$.

2) Soit $I_x = \{P \in K[X],\ P(x)=0\}$.

I_x est un idéal de $K[X]$ non nul.

Il est donc engendré par un unique polynôme unitaire Π_x qui vérifie $\forall P \in K(X)$

$$P(x)=0 \iff \Pi_x \mid P.$$

3) On a alors un isomorphisme d'anneaux $K[x] \xrightarrow{\sim} K[X]/(\Pi_x)$.

Comme $K[x] \subset L$ est intègre, on a nécessairement Π_x irréductible. En effet, si $\Pi_x = A \cdot B$ avec $\deg(A), \deg(B) < \deg(\Pi_x) = d$ on aurait dans $K[X]/(\Pi_x)$, $\overline{A}\,\overline{B} = \overline{A \cdot B} = \overline{\Pi_x} = 0$ avec $\overline{A}, \overline{B} \neq 0$.

donc $K[X]/(\Pi_x)$ serait non intègre.

Ainsi, $K[x]$ est un corps et l'on a

$$d = [K[x] : K] = [K[X]/(\Pi_x) : K].$$

Par le lemme de la base télescopique,

$$[L:K] = [L : K(x)]\,[K(x) : K].$$ d'où $d \mid [L:K] = n$.

4) Par tout i, $a_i K(x)$ est un sev de L :

en effet, soit $\alpha, \beta \in a_i K(x)$ et $\lambda \in K$, on a.

$\alpha = a_i y_1$ avec $y_1 \in K(x)$ et $\beta = a_i y_2$ avec $y_i \in K(x)$.

$$\alpha + \lambda\beta = a_i \underbrace{(y_1 + \lambda y_2)}_{\in K(x)}.$$

De plus, on a $x(a_i y) = a_i (xy) \in a_i K(x)$.

Donc $a_i K(x)$ est bien stable par M.

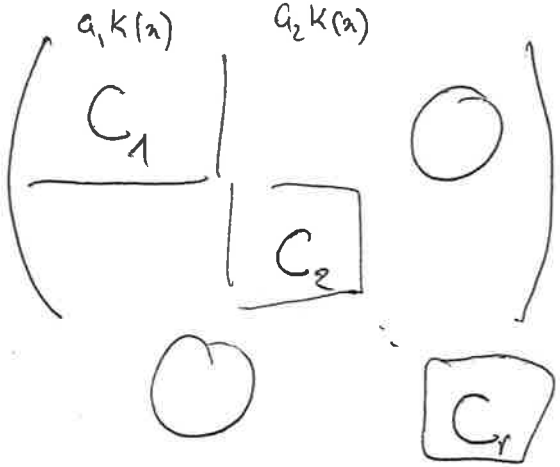
5) Par définition, $L = \overset{r}{\underset{i=1}{\oplus}} a_i K(x)$.

Choisissons $(1, x, \dots, x^{d-1})$ comme K-base de $K(x)$.

Une K-base de L est donc $\mathcal{B} = (a_1, a_1 x, a_1 x^2, \dots, a_1 x^{d-1}, a_2, \dots, a_2 x^{d-1}, \dots, a_r, \dots, a_r x^{d-1})$

Dans une telle base, la matrice de M est de la forme

$\mathrm{Mat}_{\mathcal{B}} n =$



où $C_i = \mathrm{Mat}_{(a_i x^j)} \mathrm{M}_{a_i K(x)}$.

Notons $\pi_x = a_0 + \cdots + a_{d-1} x^{d-1} + x^d$.

Mais $C_i = \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & \\ 0 & & 1 & -a_{d-1} \end{pmatrix} = C(\pi_x)$ (matrice compagnon).

(car $x \cdot a_i x^j = a_i x^{j+1}$ si $j \leq d-2$.

et $x \cdot a_i x^{d-1} = a_i x^d = -a_i \left(\sum_{k=0}^{d-1} a_k x^k \right)$)

On a alors $\chi_n = {}^{\chi}C_1 \cdots {}^{\chi}C_r = {}^{\chi}C(\pi_x)^r = \pi_x^r$.